حقوق والتزامات الدول في الحرب المعلوماتية

*مصطفى نعوس**

ملخـــص

تتمثل حرب الفضاء الإلكتروني، في أشكال عدة، مما يقتضي عرض خطرها المحتمل الذي أصبح يشكل تهديداً مباشراً للسلم والأمن الدوليين. إضافة لدراسة حرب الفضاء الإلكتروني في إطار القواعد القانونية الدولية القائمة حالياً الناظمة لاستخدام القوة بغية معرفة فيما إذا كان يمكن تطبيق معاييرها على الحرب الالكترونية. وأخيرا، بمعنى آخر، هل يمكن تطبيق القواعد القانونية الحالية المتعلقة باستخدام القوة في الفضاء الالكتروني عن طريق القياس أم أن الحاجة تفرض وضع إطار تنظيمي مصمم خصيصاً يلائم 'طبيعة حرب الفضاء الإلكتروني.

الكلمـــات الدالـــة: حرب الفضاء الإلكترونية، السلم والأمن الدوليين، استخدام القوة للدفاع عن النفس.

المقدمـــــة

تعد المعرفة والمعلومات منذ الأزل بمثابة القوة التي لا تقهر في التاريخ البشري[1]، فقد دفعت التقانة الحديثة[2] خاصة في مجال الكمبيوتر وشبكات الانترنت الدول إلى التقدم السريع في كل المجالات الحيوية، إلا أن الدور الأهم الذي تلعبه حالياً في إجراء التحول الجذري في شؤون الأمن القومي، حيث أدخلت المجتمع الدولي في حقبة جديدة في مجال حرب المعلومات[3]، والتي تعتبر الآن من أبرز أنواع القوة[4]، في العقد الماضي تمكن أحدهم من نشر Love Bug and Sasser Viruses فيروس الحب وفيروس ساسر إلى أكثر من مليون ونصف مليون جهاز كمبيوتر[5] على التوالي في أقل من أربع ساعات, وبسرعة أكثر بكثير من إمكانية أي دولة في العالم في الدفاع عن نفسها من الدمار الذي قد يلحق بها، وسبق أن أوضحت أكثر من عشرين دولة، من بينها الولايات المتحدة وروسيا والصين واستراليا وبعض من دول الاتحاد الأوروبي عن عزمها على الاندماج التام في حرب المعلومات بوصفها رد غير متكافئ في أي صراع في المستقبل قد تكون طرفاً فيه[6] والأمثلة على حروب الفضاء الالكتروني التي حدثت في السابق وتحدث الآن هي خير دليل على ما نبحث فيه، فقد استهدفت جرثومة إلكترونية أجهزة الكمبيوتر عائدة للمنشآت النووية الإيرانية مما أدى إلى تعطيل 45 ألف جهاز يقع 60 بالمائة منها داخل المنشآت النووية الإيرانية، خاصة تلك التي تعمل في إنتاج المياه الخفيفة في بوشهر في محاولة من الكيان الصهويني لشل القدرة الإيرانية على إنتاج سلاح نووي حيث لم تكن العملية الإسرائيلية ضد إيران الأولى من نوعها لمفاعل بوشهر2010، وكذلك الصين وتايوان في عام 2002، وفي عمليات حفظ السلام الدولية "عملية Belisi" التي تقودها قوات الدفاع الاسترالية عام 2001، **علماً بأن قوات السلام الدولية قد نشرت في إقليم تيمور الشرقية في اندونيسيا**، فقد سبق للاتحاد الروسي أن شن حربا إلكترونية ضد استونيا في عام 2007 وأصابت وزاراتها ومصارفها ودوائر الأمن فيها بالشلل.ثم شنت هذه الحرب على جورجيا في عام 2008، وتمكن الروس من التشويش على الاتصالات بين القيادة العسكرية والوحدات التي كانت تقاتل القوات الروسية. كما تمكنوا من تضليل الطيران الجورجى، الأمر الذي أدى إلى الهزيمة التي لحقت بها رغم كل الدعم والمساعدة التي كانت تتلقاها جورجيا من الولايات المتحدة وإسرائيل وحلف شمال الأطلسي. وفى مايو من عام 2007، تمكن الصينيون من اختراق جهاز المعلومات الإلكتروني الخاص في مكتب المستشارة الألمانية أنجيلا ميركل. كما تمكنوا من اختراق أجهزة عدد من الوزارات الألمانية بما فيها وزارة الصناعة ووزارة الدفاع! تمكن الصينيون كذلك، حسب المعلومات الرسمية الألمانية من ضخ 160 ميجابايت من المعلومات السرية قبل أن ينكشف أمرهم. وقد اتهمت ألمانيا الجيش الصيني بارتكاب تلك العمليات.حتى الولايات المتحدة التي تعتبر رائدة في الدفاع عن شبكة معلوماتها السرية، تعترف وزارة خارجيتها بأنها تتعرض لمحاولة الاختراق بمعدل

* محام، نقابة المحامين، حلب، سورية. تاريخ استلام البحث 2010/7/11 وتاريخ قبوله 2013/4/13.

مليوني مرة في اليوم الواحد. وأنه في كل جزء من الثانية يتعرض أحد المواقع الإلكترونية الرسمية إلى محاولة الاختراق.ومن خلال السلاح الإلكتروني يستطيع «العدو» أن يخرب شبكة الاتصالات العسكرية والسياسية وأن يشل الدورة الاقتصادية المالية والتجارية والصناعية وأن يعطل شبكة المواصلات... الخ. كل ذلك من دون أن يطلق رصاصة واحدة. لقد أعدت إسرائيل نفسها لهذه الحرب كما تشير إلى ذلك العملية التي استهدفت إيران. ونتساءل هنا عن إعداد الدول العربية نفسها أيضا للدفاع... وللهجوم عندما تقتضي الضرورة؟ ففي عالم يزداد اعتمادا مدنيا وعسكريا على الشبكة الإلكترونية، فإن استهداف الشبكات الوطنية الداخلية يلحق بالدولة المستهدفة خسائر كارثية ويدفعها إلى الشلل والانهيار بسرعة ومن دون قتال. من أجل ذلك، تداعت الدول الكبرى الإلكترونية في العالم وهى الولايات المتحدة والصين وروسيا والاتحاد الأوروبي إلى البحث في إعداد معاهدة جديدة تحظر استخدام السلاح الإلكتروني تكون مماثلة في جوهرها لمعاهدة حظر استخدام السلاح النووي، لما يمكن أن يلحق هذا «السلاح النظيف من خراب ودمار وشلل بالحياة المدنية العامة[7]، ونظراً لأن شبكة الانترنت تُكون حالياً ترابطاً عالمياً بين نظم المعلومات الحديثة في كل دول العالم، وتتميز بالسرعة العالية، فإن هذا ما جعل جميع البوابات مفتوحة ويمكن من خلالها للجميع الدخول غير المأذون به[8]، وتقتضي الحكمة أن تَحذر الدول من جميع الفيروسات وهجمات القراصنة المتوقعة لان أفعالهم الإجرامية غدت عمليات حرب معلوماتية حقيقية، وتبرز ضرورة اتخاذ كل الخطوات اللازمة لتفادي هذه المخاطر في أسرع ما يمكن، مما يقتضي تحديد مصدر الهجمات وتتبعها، وملاحقة فاعليها أينما كانوا ومحاسبتهم، أو الرد عليهم باستخدام القوة في ممارسة حق الدفاع عن النفس، وتبعاً لذلك، نعتقد أن المعايير القانونية القائمة حالياً فيما يتعلق باستخدام الدولة لحق القوة[9] لم تثبت بشكل كاف في تنظيم مثل هذه الحالات الفريدة والقلقة جداً[10] من حرب المعلوماتية. وكما يقول الفقيه أنطوني داماتو: أعتقد أن هناك نوعاً من روح القانون الدولي، وهذه الروح هي التطورية. وإدراكا منا لأنها تعطينا أساسا للتوقع كيف يمكن لقواعد القانون الدولي أن تتغير لتتناسب مع الأوضاع الجديدة[11]. وقد نصح البروفيسور يورام دنشتين Yoram Dinstein [12] بعقد مؤتمر دولي لتحديث القواعد القديمة الإنسانية للحرب، وأن القواعد الحالية من نوع التشريعات الدولية سوف تخدمنا جيدا إذا كان لنا ما يكفي من تطبيقها كما هي مكتوبة. إلا إننا نميل مع الاتجاه الذي يدعو إلى تطوير القواعد الدولية مع الأوضاع الجديدة. وعلى ما يبدو فإن هناك حاجة للحصول على إجابات تستند إلى مبادئ وقواعد القانون الدولي[13] هذه النوع من الأسئلة قد طرحها من بعض الفقهاء[14] الذين توقعوا إمكانية استخدام الفضاء الالكتروني كساحة معركة في القرن الواحد والعشرين. وبناءً على ما تقدم، سنقوم بتقسيم هذه الدراسة إلى أربعة مطالب كما يلي:

المطلب الأول: حرب المعلومات والدفاع المشروع

المطلب الثاني: أهم الوثائق القانونية التي تدعم حق الدولة في استخدام القوة

المطلب الثالث: إيجاد تنظيم قانوني جديد لتنظيم حرب المعلومات

المطلب الرابع: دور المؤتمرات والاتفاقيات الدولية والمنظمات الدولية في تنظيم حرب المعلومات في الفضاء الالكتروني

المطلب الأول
حرب المعلومات والدفاع المشروع

تدخل المجموعة الأولى من المبادئ القانونية التي تتعلق بتنظيم حرب الفضاء الإلكتروني في مجال القواعد القانونية الدولية الحديثة، وبشكل عام في إطار القانون الدولي العرفي[15]. تتأصل المعايير القانونية الدولية الحديثة في مجال الدفاع عن النفس أساساً في ميثاق الأمم المتحدة التي تطبق على جميع الهجمات العدوانية التي قد ترتكبها إحدى الدول أو أحد الكيانات والتنظيمات من غير الدول. ونتيجة لذلك، فإن الهجمات العدوانية المتمثلة في الحرب الإلكترونية التي قد تبدأها بعض الأطراف من الدول أو من غير الدول، لن تدخل في إطار الأحكام المنصوص عنها في ميثاق الأمم المتحدة حتى إذا ثبت تورط أي طرف مباشرة أو بشكل غير مباشر في تنفيذ مثل هذه الهجمات. بالإضافة إلى ذلك، ووفقاً للمادة 51 من الميثاق، يتعلق الإطار التنظيمي من ميثاق الأمم المتحدة فيما يتعلق بأعمال الدفاع عن النفس فقط بالقوة التي تصنف على أنها هجوم مسلح[16]. بينما قد لا يكون التسلل إلى أجهزة الكمبيوتر غير المصرح به كبيراً ومن القوة بما يكفي لتصنيفه ضمن بند "الهجمات المسلحة"، ولا بد أن يقع هجوم مسلح حتى يندرج في ظل أحكام ونصوص ميثاق الأمم المتحدة[17] وقد يكون من الصحيح الاستنتاج القائل بأن الإشارات الإلكترونية لا تشبه القنابل والرصاص، أو قوات أو أي نوع من الأنواع الأخرى من الأسلحة التقليدية. لذلك نرى،أن المجتمع الدولي لم يكن لديه أية مشكلة في اعتبار استخدام الأسلحة الكيميائية أو البيولوجية من كونها تقع تماما

ضمن تعريف الهجوم المسلح، على الرغم من كونها غير قابلة للكشف بواسطة الحواس البشرية المجردة. وهذا يتفق مع وجهة النظر التي تؤيد، أن الأسلحة المستخدمة من قبل مرتكب الهجوم المسلح أمر لا أهمية له، كون المادة 51 لا تشير إلى استخدام أية أسلحة محددة، وهذا الأمر ينطبق على أي هجوم مسلح بصرف النظر عن نوع الأسلحة الموظفة في ذلك الهجوم. لذلك ووفقا لصياغة المادة 51، فإن المجتمع الدولي سيوافق على القبول مستقبلاً اعتبار الهجوم بالأسلحة المعلوماتية يشكل هجوماً مسلحاً تبعاً لنتائجه المحتملة، وبغض النظر عن الآلية المستخدمة في إحداث هذه النتائج. لأنه في حالة وقوع هجوم معلوماتي مركز سينجح في إغلاق نظام مراقبة الحركة الجوية للدولة مثلا بالإضافة إلى إغلاق الخدمات المصرفية والنظم المالية وكذلك المرافق العامة، وكذلك يمكن أن يشمل تأثير الحروب المعلوماتية مثلا على فتح الباب على مصراعيه للسدود المغلقة الكترونياً الأمر الذي يتسبب بحدوث فيضانات عامة حادة، ووقوع الآلاف من القتلى المدنيين نتيجة لذلك ووقوع خسائر وأضرار بالممتلكات العامة والخاصة.

إن الميزة الأساسية في ميثاق الأمم المتحدة هي اللغة المحددة التي استخدمها واضعو تلك المواد فيما يتعلق بتنظيم الظروف الدقيقة التي بموجبها يحق للدول اللجوء إلى القوة المضادة، وأهم عنصر فيها، هو تفويض مجلس الأمن بتفسير مصطلح الهجوم المسلح، وفي الوقت نفسه استخدام مصطلح الهجوم المسلح يعني القبول به والأمر الذي أشير ي تفسيرها بشكل صحيح من قبل محكمة العدل الدولية في قضية نيكاراغوا، حيث يفسر قرارها بأنه لا يوجد صك قانوني قادر على تنظيم جميع الجوانب المتعلقة بأي حق قانوني معين أوفي وصف حالته الراهنة بشكل كامل ومباشر. وهذا مما يعطي مجلس الأمن صلاحيات واسعة عند التعاطي مع مسألة حرب المعلومات.

ولقد واجه المجتمع الدولي حالات مماثلة في الماضي مع ظهور الابتكارات التكنولوجية فيما يتعلق بمسألة تنظيمها مثل الطائرة، والأسلحة البيولوجية والكيميائية، وأخيراً الانشطار النووي. إلا أنه تمكن من وضع حد لها وتنظيمها, وجعلها أداة فعالة للغاية في حفظ السلم أو الحرب، وكانت بعض الأسلحة مثل الطائرات الحربية والمواد الكيميائية موضوعاً للتنظيم القانوني الدولي فيما يتعلق بآثارها المدمرة المحتملة إذا استخدمت كوسيلة للحرب.

إذ يتحتم على جميع القواعد القانونية أن تتكيف وأن يتم تطويعها لتتلاءم بشكل مستمر مع الظروف الجديدة، وبعبارة أخرى و كما يرى الأستاذ كلسن أن تكون هذه القواعد مرنة بما فيه الكفاية للتعامل حتى مع كل الحالات والظواهر الجديدة.

ونضيف إن ميثاق الأمم المتحدة يمنع استخدام القوة بين الدول وفقاً للمادة 2(4)[18] من الميثاق التي تنص على أنه "يمتنع على أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة." وأكد الفقه القضائي هذا الأمر في عدة قرارات لمحكمة العدل الدولية في فتواها في عام 1996 بشأن مشروعية التهديد أو استخدام الأسلحة النووية، وكذلك الفتوى في قضية قناة كورفو[19].

ويفهم من هذه الصيغة الواسعة لهذه المادة من الميثاق أن هذا الحظر شامل لأي استخدام أو تهديد باستخدام القوة من دون أي استثناء على الإطلاق، بما في ذلك الأعمال التي تعتبر أقل ضخامة من الحرب الشاملة، وكذلك تلك التي قد تقع خارج نطاق التعريف التقليدي للهجوم المسلح. وهذا النطاق خاص بحكم المادة 2 (4)، ولقد تم توضيحها بالإجماع من قبل الجمعية العامة للأمم المتحدة في القرار 2625[20] المتعلق بإعلان مبادئ القانون الدولي حول علاقات الصداقة والتعاون بين الدول والقرار 3314[21] المتعلق بتعريف العدوان، حيث اندمجت العبارات الواردة في المادة 2 (4) من الميثاق مع قرارات الجمعية العامة 2625 و3314 على أن السمة الرئيسية للمرحلة التي يستطيع مجلس الأمن التدخل فيها هي التي يكون فيها "الفعل المجرم" عملاً من شأنه أن يشكل تهديداً للأمن والسلم الدوليين، ويعتبر بالتالي غير قانوني، وهنا نلاحظ انه حتى يعتبر الانتهاك واضحاً للقانون الدولي في موضوع حرب المعلومات ,يجب أن يشكل الفعل تهديداً للأمن والسلم الدوليين، وينفرد نص الميثاق هنا باهتمامه بالنتائج الحاصلة وليس بالوسائل المعتمدة لتحقيق مثل هذه النتائج والتي يستخدمها الجناة مرتكبو الفعل. لذا فهو يقف على السبب الذي يمكن أن يكون هناك عمل قسري ويعفيه قانونا من النظام الرقابي عليه وفقاً لأحكام المادة 2 (4) فلمجرد كون هذه الهجمات ذات طبيعة تكنولوجية متقدمة وأدت إلى نتائج وخيمة بدولة ما، نرى أن تعتبر أعمالاً تدخل في نطاق الأفعال التي من شأنها أن تشكل تهديداً للأمن والسلم الدوليين، ويمكن تطبيق القواعد القانونية المنصوص عليها في القانون الدولي على حرب المعلومات[22] ويوجد نوعان من الاستثناءات الواردة على الحظر العام لاستخدام القوة المنصوص عنها في المادة 2 (4) من الميثاق هما تدخل مجلس الأمن، وحالة الدفاع المشروع.

الفرع الأول
قرار مجلس الأمن بالتدخل

ويتجسد الاستثناء الأول: في المادة 39[23] من ميثاق الأمم المتحدة التي تسمح لمجلس الأمن أن يقرر بموجب الفصل السابع ما يتخذ من الأعمال في حالات تهديد السلم والأمن الدوليين ووقوع العدوان، يقرّر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع[24] عملاً من أعمال العدوان، ويقدّم في ذلك توصياته أو يقرّر ما يجب اتخاذه من التدابير طبقاً لأحكام المادتين 41 و42 لحفظ السلم والأمن الدولي أو إعادته إلى نصابه. ويفوض بالقيام بالعمل القسري وفقا للمادتين 41 و42، حيث تنص المادة 41"لمجلس الأمن أن يقرِّر ما يجب اتخاذه من التدابير التي لا تتطلب استخدام القوات المسلحة لتنفيذ قراراته، وله أن يطلب إلى أعضاء "الأمم المتحدة" تطبيق هذه التدابير. ويجوز أن يكون من بينها وقف الصلات الاقتصادية والمواصلات الحديدية والبحرية والجوية والبريدية والبرقية واللاسلكية وغيرها من وسائل المواصلات وقفاً جزئياً أو كلياً، وقطع العلاقات الدبلوماسية. والقرار 4220 اللاحق لما هو منصوص عليه في الشروط التي تعتبر واسعة للغاية من المواد سالفة الذكر، ولا سيما في المادة 42 التي تنص على: إذا رأى مجلس الأمن أن التدابير المنصوص عليها في المادة 42 لا تفي بالغرض أو ثبت أنها لم تفِ به، جاز له أن يتخذ بطريق القوات الجوية والبحرية والبرية من الأعمال ما يلزم لحفظ السلم والأمن الدولي أو لإعادته إلى نصابه. ويجوز أن تتناول هذه الأعمال المظاهرات والحصر والعمليات الأخرى بطريق القوات الجوية أو البحرية أو البرية التابعة لأعضاء "الأمم المتحدة"، حيث لا توجد قيود من أي نوع فيما يتعلق بدقة طبيعة "التدابير القسرية" التي قد يتخذها بها مجلس الأمن[24]. وبناء على ذلك، يمكن السماح بإتخاذ الإجراءات القسرية"، في مجال حرب الفضاء الإلكتروني، وتقع كذلك ضمن حدود العمل المسموح بها للأحكام ذات الصلة من القرار 4222[25].

الفرع الثاني
حق الدول في الدفاع الفردي أو الجماعي

والاستثناء الثاني الوارد في ميثاق الأمم المتحدة هو الحق في الدفاع الفردي والجماعي عن النفس على النحو المبين في المادة 51 التي تنص على: ليس في هذا الميثاق ما يُضعف أو يُنقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "الأمم المتحدة" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلَّغ إلى المجلس فوراً، ولا تؤثر تلك التدابير بأي حال فيما للمجلس - بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق - من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه، إذن ليس في هذا الميثاق ما يُضعف أو يُنقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء" الأمم المتحدة" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلَّغ إلى المجلس فوراً، ولا تؤثر تلك التدابير بأي حال فيما للمجلس - بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق - من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه. وينبغي عدم تفسير مصطلح "المسلحة" في نص المادة على أنه تقييداً لاستخدام الحق لأنه من المهم أن نأخذ هذا في الاعتبار لأن المادة 51 لا تعرض الحق في الدفاع عن النفس لأول مرة في الميثاق، ولكنه تكرسه لأنه هو حق معترف به منذ فترة طويلة، ويعتبر مفهومه في الواقع أوسع بكثير من الصيغة التي يستخدم بها في نص هذه المادة[26]. وهذا يتطابق مع المفهوم الحقيقي الفعلي للهجمات المسلحة، والتي في معظم الحالات لا تشمل فقط الأسلحة العسكرية التقليدية والتكتيكات.

تعتبر عمليات حرب المعلومات حالياً المثال الحي لشكل من أشكال الهجوم المسلح التي تم تطويرها حديثاً، وعلى الرغم من كونها قادرة على إحداث دمار واسع النطاق إلا أنه حالياً لا يشملها التعريف التقليدي للمصطلح "هجوم مسلح". في الواقع، بقدر ما يتعلق الأمر بحرب الفضاء الإلكتروني، ومن خلال استعراض صيغة المادة 51، فإن السؤال الحاسم هو ما إذا كان يمكن إدراج مفهوم "هجوم حرب المعلومات" تحت تصنيف الهجوم المسلح الذي يبرر اللجوء إلى العمل الدفاعي القسري[27]، ومن خلال التركيز على الوسائل المستخدمة في هجوم حرب المعلومات يمكن للمرء أن يستنتج بأنه يمكن للإشارات الالكترونية أن تشبه القنابل وطلقات الرصاص والقذائف وأية أنواع أخرى من الأسلحة التقليدية إذا كان لديها نفس التأثير، والمجتمع الدولي حالياً قلق جداً من العواقب الوخيمة التي قد تنجم عن حرب الفضاء الإلكتروني، وخاصة إذا ما تسببت في إحداث خسائر بشرية[28]. ونرى أن هذا الميثاق سيكون مميزاً فيما إذا اعتبر هجوم الحرب المعلوماتية من خلال التحليل القانوني أنه يدخل ضمن

تصنيف "الهجوم المسلح".

باعتبار أن الميثاق ينظم المواد التي يحق بموجبها للدول أن تلجأ إلى استخدام القوة في الفصل التنظيمي، نرى أنه يجب ألا ينظر إليه من وجهة نظر تقييدية محضة، بل يجب أن يكون قادراً على إعادة إدراج العديد من المفاهيم الحديثة مثل مفهوم حرب المعلومات وغيرها من المفاهيم والنص عليها بالكامل وبشكل مباشر لتشمل نصوصه كافة هذه الجوانب وتغطيها بشكل قانوني سليم[29].

المطلب الثاني
حق الدول في استخدام القوة دفاعاً عن النفس في الفضاء الالكتروني

تتسم المجموعة الثانية من المبادئ القانونية بأهمية كبرى بالنسبة لتنظيم حرب الفضاء الإلكترونى فى مختلف الصكوك والوثائق القانونية الدولية التى تتضمن قواعد قانونية يمكن أن تدعم حق الدول في استخدام القوة في الفضاء الإلكتروني دفاعاً عن النفس.

الفرع الأول
حرب المعلومات وقواعد الحرب الآمرة

تعد قواعد الحرب الآمرة واحدة من أهم المبادئ الأساسية التي يمكن ان تكون قابلة للتطبيق مستقبلاً على وسائل شن حرب معلومات، حيث يبدأ تطبيق هذه القواعد من بداية بدء الأعمال العدائية بين المتحاربين[30]، وذلك بهدف أساسى يكمن فى وضع بعض المعايير الدنيا لحماية المدنيين والعسكريين من أجل منع المعاناة غير الضرورية والتدمير[31] كما كرسته قواعد القانون الدولى الإنسانى.

يحكم قانون الحرب مبدآن هما الضرورة العسكرية ومبدأ التناسب، والضرورة تستوجب بصورة قانونية فقط الأهداف العسكرية حصراً وما يتصل بها من البنية التحية الوطنية الحيوية[32]، وقد يكون هناك هجوم أحياناً على الأهداف التي ليست من طبيعة عسكرية ويكون شرعياً إذا كان هجوم الدولة المهاجمة على دولة أخرى فقط من أجل عرض مزاياها العسكرية من هذا الهجوم[33]، أو شيء من هذا القبيل، ويمكن بالتالي تطبيق هذين المبدأين على حرب المعلومات والاستفادة منهما.

هناك مبدأ إضافي من القواعد الآمرة "في الحرب" يمكن أن ينطبق مباشرة على حرب الانترنت هو "التمييز بين المقاتلين وغير المقاتلين" وهو شرط هام جداً فيما يتعلق بعمليات حرب المعلومات ويحتاج إلى أذن شرعي لإتخاذ الإجراءات القسرية أثناء وجود النزاع الدولي[34]، في حال قيام بعض الأفراد بهجوم وشن حرب الكترونية، فهؤلاء المهاجمون يقعون خارج نطاق التعريف القانوني للمقاتلين وسيصبحون أهدافاً عسكرية مشروعة، ويكونون أيضا عرضة للملاحقة الجنائية، وكذلك ترتيب مسؤولية الدولة التي ينتمون إليها وسيكونون منتهكين لقانون الحرب[35]، ويمكن تطبيق مبادئ أخرى على الحرب الإلكترونية، هي تلك التي تحظر استخدام الأسلحة التقنية ووسائل الحرب التي يمكن أن تسبب إصابات زائدة ومعاناة لا داعي لها وتلحق أضراراً في المدى البعيد إلى البيئة[36] إن تطبيق هذا المبدأ خاصة في عمليات الحرب الإلكترونية له أهمية خاصة، حيث تتعرض مجموع شبكات المعلومات الحديثة المترابطة لأضرار جانبية بشدة، والتي قد تكون ناجمة عن أسلحة الحرب الإلكترونية التي تستخدم عشوائياً[37]، ونرى أنه سيكون ملزماً التحديد القانوني بأن أيا من هذه الوسائل محظورة بأي شكل من الأشكال من قبل القانون الدولي[38]، تحتاج عمليات حرب المعلومات أيضاً إلى الامتثال للقواعد الآمرة "في الحرب" التي تقضي بإعمال مبدأ الفروسية والشرف وعدم اللجوء إلى أسلوب الغدر، مهما كانت التقنيات الحربية المستخدمة فلا يجوز استخدامها[39].

المبدأ الأخير من "قواعد الحرب الآمرة" الذي ينطبق على عمليات حرب المعلومات هو مبدأ الحياد الذي ينص على: أولا، يلزم المحاربون قانونا باحترام حقوق وأراضي الدول المحايدة في أي صراع بينهما، وثانيا، منع الدول المحايدة بكل الوسائل الضرورية، بما في ذلك استخدام القوة، من استخدام أراضيها من قبل أحد الأطراف المتحاربة، وثالثا، الامتناع على الدول المحايدة عن تقديم المساعدة بأي طريق للأطراف المتحاربة. وتكمن أهمية هذه القاعدة القانونية لا سيما فيما يتعلق بالحرب الإلكترونية في أن المعتدين المحتملين من المرجح أن يكونوا دائماً متخفين عند الهجوم الالكتروني ويوجهون ضرباتهم من خلال واحدة من شبكات المعلومات المتصلة والموجودة في أكثر من دولة وقد تتدخل أحياناً بعض الدول المحايدة للمساعدة بدون موافقة أو معرفة الدول الأخرى أو شيء من هذا القبيل.

الفرع الثاني
حرب المعلومات وقانون الفضاء الخارجي

هناك فرع آخر في القانون الدولي يمكن أن يضم عدداً قليلاً من القواعد القانونية القابلة للتطبيق على الحرب الإلكترونية هو قانون الفضاء. ينبع هذا الانطباق أساساً من

حقيقة أن الشبكات العالمية، والجوانب الرئيسية لتكنولوجيا المعلومات الحديثة، تعتمد على منصات فضائية متعددة تدور حول الأرض من أجل دعم المحطات الأرضية[40] وفضلا عن ذلك، تعتبر هذه المنصات الفضائية في غاية الأهمية في عمليات حرب المعلومات وذلك لسببين الأول: تعتبر هذه المنصات من العناصر الأكثر ضعفاً في نظام المعلومات لأنه يستحيل صد أي هجوم قد يقع عليها، والثاني، أنها كذلك تمثل القوة الأكثر حيوية ومقدرة لأي دولة تريد القيام بعمليات حرب معلوماتية بشكل ناجح، وبالتالي ستكون هذه المنصات الفضائية مشتركة بالضرورة في صلب أي حرب معلوماتية رئيسية معاصرة سواء لعملية دفاعية أو هجومية[41]. وبالتالي يمكن أن تندرج عمليات حرب المعلومات في إطار القواعد القانونية التي تنظم الأنشطة في الفضاء والتي صيغت في الغالب في معاهدة الفضاء الخارجي منذ عام 1967[42] إذ تعد هذه المبادئ معتمدة وملزمة في المجتمع الدولي وتعتبر من قبيل القانون[43] الدولي العرفي. أولا وقبل كل شيء، حيث لا تزال أنشطة حرب المعلومات في الفضاء الخارجي تخضع للإطار القانوني القائم حالياً الذي ينظم استخدام القوة. ثانيا، مشاركة جميع الدول في أنشطة حرب المعلومات في الفضاء الخارجي يتوجب الامتناع عن التسبب في أي تدخل يمكن أن يكون ضاراً مع أنشطة الدول الأخرى. ثالثا، تتحمل الدول المشاركة في أنشطة حرب المعلومات المسؤولية الدولية عن جميع هذه الأنشطة التي تقوم بها في الفضاء الخارجي، وبغض النظر عن ما إذا كانت هذه الأنشطة تقوم بها الحكومات أوالكيانات الأخرى غير الحكومية ونستطيع أن نأخذ مثالين من الصكوك التنظيمية المتخصصة في القانون الدولي للفضاء الخارجي مع التطبيق المباشر على عمليات حرب المعلومات[44] هي اتفاقيات انتلسات[45] واتفاقيات إنمارسات[46].

الفرع الثالث
حرب المعلومات، وقانون البحار

نصت اتفاقية الأمم المتحدة لقانون البحار لعام 1982 على عدة قواعد قانونية يمكن أن تنطبق على أنشطة حرب المعلومات[47]. أولها، إن الاتفاقية تنص على أن جميع السفن البحرية تستطيع استخدام حق المرور البريء في المياه الإقليمية للدولة ويجب الامتناع عن المشاركة في الأنشطة التي تضر بالسلام وحسن النظام والأمن في الدول الساحلية. حيث يمكن لكل واحدة من سلسلة قوائم الاتفاقية المحددة للأنشطة "الضارة" أن تكون جزءاً رئيسياً لا يتجزأ من عمليات الحرب الإلكترونية[48]. وعلاوة على ذلك، تدعو الاتفاقية جميع الدول للتعاون في مجال قمع البث غير المصرح به من أعالي البحار[49] في حين يستغرق أيضا عدة خطوات لضمان ملاحقة مرتكبي البث غير المصرح به من أعالي البحار. وأخيرا، فإن الاتفاقية تنص أيضاً على حماية الكوابل الغواصة. وإن أهم النصوص التي نصت على عدم السماح بالبث لبرامج الراديو في أعالي البحار تجلى في المادة 9 من الاتفاقية.

الفرع الرابع
حرب المعلومات وقانون الاتصالات

يعد قانون الاتصالات فرعاً من القانون الدولي الذي يمكن أن تطبق قواعده القانونية على عمليات حرب المعلومات. ويجري تعيين هذه القواعد القانونية المنصوص عليها في الاتفاقية الدولية للاتصالات[50] حيث تسمح الاتفاقية بقطع أي اتصالات سلكية أو لاسلكية التي قد تظهر بأنها قد تشكل خطراً على أمن أي دولة طرف في الاتفاقية وعلاوة على ذلك، يحق للدول تعليق جميع خدمات الاتصالات الدولية لمدة غير محدودة لأسباب تتعلق بالأمن الوطني، وإنها تقوم على الفور بإخطار الأمين العام للأمم المتحدة. وينبغي بالإضافة إلى ذلك، وضع جميع المحطات اللاسلكية وتشغيلها بطريقة لا تتسبب بتداخلات ضارة للغير. في نهاية المطاف، وكما هو منصوص عليه وحرب المعلومات ذات الصلة، يحق الدول الأطراف في الاتفاقية الاحتفاظ بحرية مطلقة فيما يتعلق احتمال استخدام منشآتها الاتصالاتية العسكرية ما دامت تتخذ جميع الخطوات اللازمة لمنع أي تدخل ضار.

الفرع الخامس
حرب المعلومات والقانون الدولي الإتفاقي

يعد قانون المعاهدات من أهم الفروع في القانون الدولي الممكن تطبيق قواعده على عمليات حرب المعلومات ويرجع ذلك إلى أن المعاهدات تمثل الوسيلة الأساسية التي يتعامل بها أعضاء المجتمع الدولي في مختلف المجالات فيما بينهم[51]. وفي حال قيام الحرب ثمة تساؤل يطرح هل بالإمكان تطبيق أحكام المعاهدة بين الدول المتحاربة في زمن الحرب. فعندما لا يتم ذلك عندها سيكون الموضوع رهناً "بقواعد الحرب الآمرة" وبالتالي يمكن تطبيق قواعد الحرب على خرب المعلومات كما أشرنا أعلاه[52]. وعند تطبيق أحكام الاتفاقيات والمعاهدات يمكن أن تكون هناك بضعة جوانب من قانون الاتفاقات الدولية التي يمكن تطبيقها بشكل مباشر على سير

عمليات حرب المعلومات[53]. مثل معاهدات تسليم المجرمين، وكذلك على اتفاقيات المساعدة القضائية وهي الأكثر أهمية، خاصة التعاون بين الدول في الوسائل المتاحة فيما بينها لاتخاذ لإجراءات صارمة ضد مرتكبي جرائم التسلل إلى أجهزة الكمبيوتر التى تبدو وكأنها غير مصرح بها فى معظم الدول، ولأنه فى الحالات التى يكون فيها (التسلل للكمبيوتر غير مصرح به) غير محدد بوصفه عملاً إجرامياً، ستحجم الحكومات عن تقديم مثل هذه المساعدة القضائية في جميع الأشكال المتعلقة به وهذا ما ساهمت في تحديده وتوضيحه الاتفاقية الأوربية للجرائم المرتكبة عبر الانترنت 2001 من خلال تحديد الإجراءات وآليات التعاون بين الدول في مجال مكافحة الإجرام عبر الانترنت[54] وبالتالي، فإنه من الأهمية الكبرى تصور كل من الأنواع المذكورة أعلاه من المعاهدات في مثل هذه الطريقة وكأنها تغطي بعض أنشطة حرب المعلومات، سواء من خلال توسيع هذه الاتفاقيات بما فيه الكفاية لتدارك الموقف المطلوب، أو من خلال إدراج أحكام محددة تهدف إلى تنظيم الحرب الإلكترونية.

تشمل الاتفاقيات الدولية التي تنظم الطيران المدني أيضاً أحكاماً تنظم سلوك حرب المعلومات. أولا، تعتبر جميع الدول ملزمة، في جميع الظروف، بمراعاة الشروط الواجب توافرها من أجل سلامة الملاحة بالنسبة إلى الطائرات المدنية وعدم التدخل بأي شكل من الأشكال في السلامة الأمنية لها، ويحظر على الدول اللجوء إلى استخدام جميع أنواع الأسلحة ضد الطيران المدني. وعلاوة على ذلك، وكما هو منصوص عليه في المعاهدات التي تنظم العلاقات الدبلوماسية، يجب على أعضاء المجتمع الدولي عدم المشاركة بأي شكل في أنشطة حرب المعلومات التي تنال من الموظفين الدبلوماسيين أو المباني أو المعدات، وأن تأخذ في الاعتبار الموظفين الدبلوماسيين أو المباني أو المعدات لا يمكن أن تكون هدفا لأي من هذه الأنشطة، لأنها لا تستخدم إلا بما يتفق مع الأغراض الرسمية بشكل دقيق[55] وتمثل الاتفاقيات النوع الأخير من الاتفاقات الدولية التي تتحمل صلة مباشرة بتنظيم عملية حرب المعلومات. وتشترط هذه الاتفاقيات جعل جميع عمليات حرب المعلومات التي قد تبدأها القوات العسكرية المرابطة في الخارج للشروط القانونية التالية: (أ) ما إذا كانت الدولة المضيفة قد قامت بالإخطار قبل البدء بأي عملية حرب معلومات، (ب) ما إذا كانت المعدات الفعلية التي تنطوي عليها أية معلومات معينة سوف تكون العملية الحربية في خرق التزام قانوني محدد بموجب اتفاق معين، (ج) ما إذا كانت حرب المعلومات الواردة العملية تتطلب استخدام الدولة المضيفة لنظم المعلومات الخاصة بها، (د) وأخيرا، إذا كان الشروع في عملية الحرب على معلومات من الدولة المضيفة جعل هذا الموضوع ولا سيما الدولة المضيفة لأعمال انتقامية محتملة. ورغم أن الغالبية العظمى من الصكوك القانونية الدولية الحديثة لا تحتوي إلا على عدد قليل جدا من الأحكام التي تنطبق على الجوانب الأوسع لعمليات حرب المعلومات، ولا يزال هناك عدم وجود إطار قانوني دولي موجود خصيصاً لتنظيم هذه الظاهرة الناشئة. سيبقى التهديد مستمراً، في حال عدم وجود إطار قانوني دولي معتمد عالمياً يقوم بتنظيم حرب المعلومات عبر السنوات القادمة، لان هذا التنظيم سوف يلزم الدول بتوحيد قواها في تقليل وخفض الأنشطة غير المشروعة في حرب المعلومات، وفي حال عد وجوده سوف يجعل أي محاولة لتوجيه الاتهام لمرتكبي مثل هذه الأنشطة لا معنى له وسيبقى معتمداً فقط على حسن نية الحكومات[56].

الفرع السادس
حرب المعلومات والقانون الدولي العرفي

لقد أكدت قبل محكمة العدل الدولية مراراً في أحكامها، إن القواعد القانونية المتعلقة بحق الدول في استخدام القوة في الدفاع عن النفس ليست مبنية فقط على أساس ميثاق الأمم المتحدة ولكن أيضا على مبادئ القانون الدولي العام العرفي.

حيث يمكن اعتبار الإجراءات التي اتخذت في الدفاع عن النفس شرعية فيما إذا كانت تخضع لشرطي الضرورة والتناسب، وهما الشرطان اللذان يجب أن يكونا متلازمين مع ضرورات الدفاع في مفهوم الدفاع عن النفس. ويبدو أن "مبدأ كارولين" الذي أنشأه السيد دانيال وبستر في 1841 قد نجح في صياغة الاختبار النهائي لأية دولة، في اعتبار الإجراءات القسرية المتخذة من قبلها مشروعة في مفهوم الدفاع عن النفس في حال انطباق شرطي هذا المبدأ، لذلك نرى أنه يمكن الاستفادة منه وتطبيقه على التصرفات المستقبلية للدول في حرب المعلومات.

وهذا المبدأ معترف به منذ أكثر من قرن ونصف تماماً على انه من القواعد القانونية الدولية العرفية وهو "مبدأ كارولين"، والذي يسمح للدولة اللجوء إلى القوة لأغراض الدفاع عن النفس بالاستناد إلى شرطي الضرورة، والتناسب والموازنة في استخدامها، وبصرف النظر عما إذا كان اللجوء إلى القوة قد تم باستخدام الوسائل التقليدية للحرب أو الحديثة منها أم بوسائل تقنية حديثة تم تطويرها حديثا.

وبالتالي يمكن لأعضاء المجتمع الدولي الذين يجدون أنفسهم في وضع يضطرهم للدفاع عن النفس المراعاة قدر المستطاع لشروط "مبدأ كارولين" المؤسس على شرطي الضرورة والتناسب (قياساً على المبدأ الفقهي الشرعي القائل بأن الضرورات تقدر بقدرها) وبالتالي إمكانية الدول لاستخدام القوة في الفضاء الإلكتروني للدفاع عن النفس من دون أي ارتكاب أي خرق لميثاق الأمم المتحدة، وبالتالي تظهر وكأنها تعمل بصورة قانونية وتمارس سيادتها استناداً لمبدأ "الاختصاص المكاني" وفي ممارسة لحقها الطبيعي في الدفاع عن النفس، شريطة الالتزام كذلك ب "قانون الحرب". في الواقع، ليست هناك أية وسيلة ممكنة للتنبؤ بأي شكل من الأشكال بالضبط التي يمكن فيها أن تتطور فيها حرب المعلومات، وما هي الإمكانيات المتاحة لشبكات الكمبيوتر المنتشرة على نطاق واسع؟ وكيف يمكن أن يتم الهجوم على الشبكات منها أو عليها تماماً؟ وفوق كل ذلك كيف يمكن للمجتمع الدولي أن يتجه نحو تطبيق القواعد القانونية الدولية القائمة المتعلقة بتنظيم استخدام القوة بشكل عام؟ والقواعد العرفية على وجه الخصوص؟ في مجال حرب المعلومات؟ كل ذلك دفع دول العالم الآن إلى البحث عن آليات تنظيم جديدة يقوم بالاستفادة من المعطيات السابقة والقيام بالمهمة الموكولة إليه.

المطلب الثالث
حرب المعلومات، والحاجة إلى إيجاد تنظيم جديد

يحتاج القانون الدولى إلى إضافة تشريعات جديدة لسد الثغرات القانونية والاستفادة كذلك من التشريعات الوضعية.

الفرع الأول
سد الثغرات القانونية

المقترح الأول: إن السمة الأولى للمقترح من هذا القبيل سوف تقوم بسد أية ثغرات فى التشريعات الموجودة حالياً[57]، وكذلك تضمن تحديث القواعد القانونية القائمة المطبقة بالفعل حالياً على أنشطة حرب المعلومات سواء كان ذلك على المستوى المحلى، من خلال اعتماد القوانين الجنائية اللازمة، أم على المستوى الدولى، من خلال اعتماد الآليات القانونية الدولية التى تكفل تقديم المساعدة القضائية المتبادلة. ويمكن الركون فى ذلك إلى المبادئ والقواعد التى أرستها الاتفاقية الأوربية للجرائم المرتكبة عبر الانترنت 2001.

الفرع الثانى
الاستفادة من التشريعات الوضعية

أما الاقتراح الثاني: فهو للاستفادة من الإطار التنظيمى القائم بالفعل الذي يضم جميع الوثائق القانونية الدولية التى تتضمن أحكاماً محددة لتنطبق على عمليات حرب المعلومات. جميع هذه الصكوك القانونية، في جميع أقسامها الخاصة، ومكافحة كل أشكال التسلل غير المشروع إلى أجهزة الكمبيوتر ونظم المعلومات، وتوجيه دعوة عامة إلى جميع الدول للتعاون فيما بينها للحد من مثل هذه الأفعال الجرمية في جميع أشكالها. عموما كالوثائق القانونية الدولية التي تقع ضمن هذه الفئة المذكورة، أو حتى التي يجري النظر فيها حالياً للتعبير عنها بمثابة قانون دولي عرفي، ومن حيث النتيجة تصبح ملزمة لجميع الدول على قدم المساواة حتى لو كانت بعض الدول ليست طرفاً في هذه الصكوك[58]. ويوجد مصلحة كاملة للدول للاستفادة من تقانة المعلومات الحديثة والدفع نحو الالتزام الصارم بالقواعد القانونية القائمة حالياً والتي تنطبق منها على أنشطة الحرب الإلكترونية.

ومع ذلك، وعلى الرغم من حقيقة أن هناك بعض الجوانب من الإطارات القانونية الدولية التي يمكن تطبيقها على المسائل التي هي حالياً في متناول اليد، إلا أن الطبيعة الخاصة جداً للانترنت تجعلها جديدة تماماً، وعلى درجة عالية من التخصص ومن الاختلاف الكلي بشدة وهذا يجعل من بعض المصالح الوطنية تتعارض مع بعضها البعض في أكثر الأحيان. ونتيجة لذلك، هناك ضرورة تدفع دول العالم حالياً للتحرك في اتجاه اعتماد صك قانوني دولي مصمم خصيصاً لتنظيم قانون للإنترنت بشكل عام، وقانون لحرب المعلومات على وجه الخصوص.

من وجهة نظر القانون الدولي، فإن السؤال الأول الذي يجب الإجابة عليه هو هل يمكن اعتبار الهجمات على شبكات الحواسيب مبرراً للدول لاستخدام القوة، أو حتى القيام بهجوم مسلح ومتى. قبل أن نحاول في أي تحليل، سيكون من الجيد أن نأخذ في الاعتبار بعض الافتراضات مثلاً فيما يتعلق بمسألة الاختصاص القضائي، هل يجب تحديد مكان نشوء الهجوم ونأخذ بالاختصاص الإقليمي أم المكان الذي ظهرت فيه نتائج هذا الهجوم "ونأخذ بمبدأ الآثار" وطبعاً سيكون، تحديد الموقع الجغرافي للمهاجمين، على درجة عالية من الأهمية وكذلك أين وقعت آثار هذا الهجوم[59] وهناك أيضا أشكال عديدة من الهجمات المحتملة، وهذا يعني ليس كل هجوم سيكون على المستوى الذي يؤدي بالدولة إلى استخدام القوة ضده. ولتوضيح هذه

الفكرة، ينبغي العودة إلى بعض الأمثلة من الهجمات التي حدثت ضد شبكات الكمبيوتر العالمية مثل الهجوم الذي حدث على بورصة نيويورك للأوراق المالية، والذي أدى إلى إغلاق الأسواق المالية، والهجوم على نظام مترو الأنفاق لمدينة نيويورك مما تسبب في اصطدام هائل وعرقلة، أو على نظام المراقبة الجوية الأمريكية الذي أدى إلى تحطم طائرة مدنية. والسؤال الذي يطرح نفسه هل مثل هذا الهجوم سيبرر لاستخدام القوة أم لا؟ في الواقع، هناك سابقة قوية مشابهة في المجتمع الدولي يمكن الركون إليها والاستفادة منها من اجل إنشاء قواعد قانونية تنطبق على حرب المعلومات "وقدمت أفضل السبل الممكنة لهذا التنظيم الخاص وهي التي ظهرت حديثا ولها من الملامح الخاصة بها جداً أيضاً وشكلت تحدياً للحدود الوطنية التقليدية، وأنها تقع بنفس الوقت في وسط مجموعة من المصالح الوطنية الهامة المتعارضة مع بعضها البعض بشدة[60] هذه السابقة تضم اثنين من الصكوك القانونية الأكثر أهمية في تاريخ القانون الدولي، الأول اتفاقية الأمم المتحدة لقانون البحار لعام 1982 والثاني معاهدة عام 1967 بشأن الفضاء الخارجي. ويمكننا بالتالي المضي قدماً في نفس العمليات المشابهة لتلك التي أدت إلى اعتماد المعاهدتين المذكورتين والتي من شأنها أن تؤدي إلى اعتماد صك قانوني دولي لمواجهة التحديات المفروضة في تنظيم الانترنت بشكل ناجح.

أولاً: سمات الفضاء الالكتروني

للفضاء الالكتروني سمات محددة لابد من مراعاتها إلا وهي

التحدي الأول: والأكثر شهرة لحرب المعلومات هو: **أ)** بدء هجوم المهاجمين يتسبب في حدوث أضرار خطيرة فور الوصول غير المصرح به إلى نظم المعلومات **(ب)** طبيعة الهجوم الخفي للغاية يجعل من الصعب جدا تحديد الموقع الدقيق للهجوم والمهاجمين وحرب المعلومات المعينة، مما يعقد عمل الضحية للجوء للعمل الدفاعي القسري واستخدام القوة، **(ج)** حرب المعلومات هي مثال حي منهجي على حقل في الدولة لا يمكن أن نأمل فيه تحقيق التفوق أو أن تجعل الدولة نفسها منيعة من الهجوم عليها. ومن شأن الفهم الكامل لهذه الميزات التأكد من أن أية قواعد تنظيمية سوف تنشأ يجب عليها تحقيق التوازن الصحيح بين الهجوم وكذلك المصالح الدفاعية لكل دول العالم فيما يتعلق بحرب المعلومات، وبالتالي ضمان على أن تكون فعالة وأن تحظى بأكبر دعم ممكن في المجتمع الدولي.

ثانياً: توافق القانون الجديد مع القواعد الدولية الحالية

وأما التحدي الثاني هو أن يتوافق ويتطابق أي صك قانوني دولي جديد مع القواعد القانونية القائمة حالياً في الدفاع عن النفس ويتعلق بتنظيم حرب المعلومات. وعلاوة على ذلك، فإن تصور أية أحكام اتفاقية مستقبلية ممكنة لتنظيم حرب المعلومات يجب أن تدرج في نصوصها قواعد "قانون الحرب" التي تتعلق بها لتستهدفها تماماً، فضلا عن وضع قواعد للتمييز بين المقاتلين وغير المقاتلين والمرتزقة. بالإضافة إلى ذلك، ينبغي أن تتخذ كل الخطوات الممكنة من أجل تفادي الإخطار المحدقة للوصول إلى مجتمع الفضاء الإلكتروني، وكذلك أيضاً لضمان الوصول بأعلى الدرجات الممكنة.

ثالثاً: سيكون التحدي النهائي الذي يواجه واضعي أي تنظيم لحرب المعلومات في المستقبل، إيلاء الأولوية في النص على الضمانات وتوفير المساعدات القضائية الكاملة بين الحكومات في حالات تعرض أحدها إلى هجمات من نوع حرب المعلومات من أجل التعرف على منشأها. ويجب على النظام القانوني المقترح أن لا يترك أدنى شك في تحديد الحالات التي يتم التعرف فيها على دولة معينة ومن دون أي شك بأنها تشكل مصدراً لهجوم أو حرب معلومات خطيرة بدقة متناهية، والحالات التي ترفض فيها الحكومات تقديم المساعدة القضائية بشأن تقديم مرتكبي الهجوم إلى العدالة، وتحديد ما إذا سيكون هناك افتراض اعتبار الدولة تشارك بالجرم والمسؤولية واحتمال القيام ضدها بعمل دفاعي قسري.

هذا التحدي الأخير على وجه الخصوص هو الأبرز من أي وقت مضى حيث يؤكد على حاجة مجتمع القانون الدولي لنموذج جديد فيما يتعلق بالتنظيم الفعال لحرب المعلومات، وجميع الإجراءات القسرية المحتملة المتصلة به. ويرجع ذلك فقط إلى أن ظهور أدوات الحرب الإلكترونية والتقنيات الحديثة التي وفرت لبعض الجهات العدوانية السلاح الفعال والبسيط للغاية حتى الآن ولم يسبق لها مثيل من القوة المسلحة وعلى الرغم من كونها لا تزال في مراحلها الأولى من عملية التطور.

الفرع الثالث

حرب المعلومات وخصائصها الفريدة

إن أي محاولة للتنبؤ بأن حرب المعلومات ستشكل فى نهاية المطاف تهديداً رئيسياً للسلام والأمن الدوليين ,سيكون من السابق لأوانه فى الوقت الراهن التكهن بذلك، ولكن وبنفس الوقت تنطوي هذه الحرب على الكثير من المخاطر

والتى لا يمكن تجاهلها بحال من الأحوال. والحقيقة التى لا يمكن تجاهلها هو أن هذا المجال الواسع نفسه من شبكات المعلومات العالمية حالياً هو المسؤول عن قيادة الطريق إلى الازدهار والتنمية والرفاه لجميع أعضاء المجتمع الدولى، ويجعل بنفس الوقت من كل تلك الدول التى تحاول تحقيق الاستفادة القصوى منه، عرضة لهجمات حرب معلوماتية(61).

لا تستطيع حالياً أي دولة ذات قوة عظمى ومتفوقة سياسياً أو عسكرياً، أو اقتصادياً ان تقاوم الاستفادة من المزايا التي تتيحها الشبكات العالمية للمعلومات" أو أن تستغني عنها، وبالإضافة إلى ذلك، تستطيع أن تعتمد عليها أيضاً من أجل شن "حرب معلوماتية" ضد أعدائها "بدلا من أن تستخدم الطرق التقليدية للقوة المسلحة. نظراً للمزايا التي تجعل منها النموذج الأكثر إغراءاً لشن حرب هجمات حرب الكترونية، نظرا للصعوبة البالغة في تحديد مصدر هذه الهجمات. وخاصة أنها تستطيع الإنكار وصعوبة الإثبات ضدها بأنها من قامت بالهجوم بشكل كبير، وكذلك تتجنب قوة خصومها.

سمة إضافية فريدة من حرب المعلومات لا يمكن لأي دولة أن تتخذ خطوات دفاعية كافية ضد هذا النوع من الهجوم، ولكن يمكن أن توجد هناك فرصة في الدفاع والذود عن الحمى من خلال التعاون والتنسيق بين الحكومات فيما بينها وكذلك التعاون بين الحكومات والقطاع الخاص. وربما هذا يتناقض مع الشكل التقليدي للقانون الدولي الحالي المتعلق بقانون الحرب سواء من حيث المسؤولية عن الحرب التي تقع تحت الولاية القضائية لحكومات الدول المعينة.

تتسبب هجمات حرب المعلومات في أضرار كبيرة باستخدام أدوات وآليات قليلة جداً. ولذلك فإن الدول التي تجد نفسها تحت أي شكل من أشكال هجوم الحرب الإلكترونية عليها أن تتخذ من الإجراءات الكافية من أجل التصدي لأي هجوم، وتحييد ما تستطيع من آثارها الضارة والتعرف على مصدرها أيضا، وخاصة فيما يتعلق في مجال التجارة الالكترونية وأن تتسلح الدولة بجميع التقنيات الدفاعية من أجل ذلك.

المطلب الرابع
دور المؤتمرات والمنظمات الدولية في حماية الفضاء الالكتروني

تلعب المؤتمرات الدولية دوراً هاماً جداً في تكوين المبادئ والقواعد القانونية التي تتعلق بتنظيم أي ظاهرة جديدة تطرق باب القانون الدولي لتنظيمها، ومن المتعارف عليه أن معظم المنظمات الدولية قد نشأت في أحشاء المؤتمرات الدولية ولقد كان للمنظمات الدولية والإقليمية (كالأمم المتحدة ووكالاتها المتخصصة كاليونيسكو والاتحاد الدولي للاتصالات ومنظمة التعاون الاقتصادي والاجتماعي والاتحاد الأوربي)(62) دوراً لا يستهان به في الدعوة إلى تلك المؤتمرات. سنعرض فيما يلي لأهم المؤتمرات التي تعرضت لمسألة تنظيم الفضاء الالكتروني وبخاصة ما تعلق منها بحرب المعلومات وان التعاون بين المنظمات الدولية يساعد على رسم إستراتيجية واضحة المعالم ومنع التضارب بين الدراسات والأبحاث التي تقوم عليها الدول في هذا المجال، مما يؤدي إلى إلى إتاحة الفرصة لاستفادة الدول النامية من خبرات وتجارب الدول المتقدمة. واهم الاتفاقيات التي عقدت من أجلها:

الفرع الأول
دور المؤتمرات والاتفاقيات الدولية

لقد أسهمت المؤتمرات الدولية من خلال المبادئ والتوصيات الصادرة عنها، في تنظيم العديد من النقاط الجوهرية المتعلقة بالفضاء الالكتروني(63)، في مختلف قطاعاته، وقد ساعدت هذه المؤتمرات في وضع العديد من القواعد القانونية التي شكلت اللبنة الأولى في صرح القانون الدولي المتعلق بتنظيم الفضاء الالكتروني، وربما أمكننا أن نطلق عليه القانون الدولي للانترنت.

ومن أهم هذه المؤتمرات نذكر:

أولاً: مؤتمر القمة العالمية لمجتمع المعلومات في جنيف 2003

أمام تزايد الأخطار التي تحدث في شبكة الانترنت وخاصة ما يحدث من حروب معلوماتية، وبناء على قرار مجلس الاتحاد الدولي للاتصالات وقراري الجمعية العامة 183/56 238/57. تم عقد مؤتمر القمة العالمية لمجتمع المعلومات في جنيف – بالكسبو 2003، في الفترة من 10 إلى 12 كانون الأول 2003، تحت عنوان (بناء مجتمع المعلومات: تحد عالمي في الألفيـــة الجديدة)، ولقد حضر المؤتمر أكثر من 11.047 شخصاً يمثلون 176 دولة و100 منظمة دولية و481 منظمة غير حكومية و98 شركة خاصة و631 وسيلة إعلامية، بينما حضر 40 رئيس دولة وحكومة فقط من أصل 60 كانوا قد أعلنوا مشاركتهم. ليشهدوا ولادة المجتمع المعلوماتي الذي سيميز الألفية الثالثة، وكان هذا المؤتمر يستهدف تحقيق رؤية ومبادئ مشتركة من أجل ضمان أمن الانترنت واستمرارها واستفادة جميع البشرية من

الإمكانات التي يمكن ان تقدمها وتنميتها، وكذلك لبحث السبل لتشجيع الحكومات والمنظمات الدولية للقيام بما يجب لتحقيق هذه الأغراض، ولقد أقر رؤساء الدول الحاضرون والمنظمات الدولية بأهمية الإنترنت: وسلموا بأنها عنصر محوري في البنية التحتية لمجتمع المعلومات الناشئ، ولقد صدر عن هذا المؤتمر في ختام أعماله إعلاناً يتضمن ضرورة حماية بيئة الانترنت الافتراضية، متضمناً أول وثيقة دولية تتعلق بمبادئ العلاقات بين الدول في شأن الانترنت وكيفية التعامل معها وبالإضافة إلى خطة عمل. وإذا نظرنا إلى الإعلان نجده قد أكد في مبادئه على أهمية بناء الثقة والطمأنينة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، حيث تمخض عنه تشكيل الفريق العامل لإدارة الانترنت، الذي شكل من قبل الأمين العام للأمم المتحدة من مجموعة من الخبراء المختصين من كل الاختصاصات من أجل إعداد تقرير كامل حول إدارة الانترنت، والذي صدر قبيل انعقاد المؤتمر الثاني الذي تقرر عقده في تونس 2005.

ثانياً: مؤتمر القمة العالمية لمجتمع المعلومات في تونس 2005

افتتح السيد يوشيو أوتسومي الأمين العام للاتحاد الدولي للاتصالات المرحلة الثانية في من القمة العالمية لمجتمع المعلومات في تونس، ولقد جاء في أهم مقررات هذا المؤتمر: السعي إلى بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات والتأكيد على ضرورة المضي، بالتعاون مع جميع أصحاب المصلحة، في تعزيز وتنمية وتنفيذ ثقافة عالمية للأمن السيبراني، كما ورد في قرار الجمعية العامة للأمم المتحدة 57/239، وفي قرارات بعض المحافل الإقليمية ذات الصلة. وتتطلب هذه الثقافة إجراءات وطنية ومزيداً من التعاون الدولي لتعزيز الأمن، والعمل في الوقت ذاته على النهوض بحماية المعلومات الشخصية وحماية الخصوصية والبيانات. وينبغي أن يعزّز استمرار تنمية ثقافة الأمن السيبراني إمكانيات النفاذ والتجارة، وأن يراعي مستوى التنمية الاجتماعية والاقتصادية في كل بلد وأن يحترم الجوانب الموجهة نحو التنمية في مجتمع المعلومات، والتأكيد على أهمية ملاحقة الجرائم السيبرانية قضائياً، بما فيها الجرائم السيبرانية التي تُرتكب ضمن الولاية القانونية ولكنها تؤثر في ولايات قانونية أخرى. ودعوة الحكومات بالتعاون مع أصحاب المصلحة الآخرين إلى وضع التشريعات اللازمة للتحقيق في الجرائم السيبرانية وملاحقتها قضائياً، مع الاستفادة من الأطر القائمة، ومنها على سبيل المثال قرار الجمعية العامة للأمم المتحدة 55/63 وقرارها 56/121 بشأن "مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية" واتفاقية المجلس الأوروبي بشأن الجرائم السيبرانية. ويمكن القول بأن هذا المؤتمر قد شكل منعطفاً تاريخياً خطيراً، وكان بداية الانطلاق الحقيقية لبدء الاهتمام بالفضاء الالكتروني عموماً، ومازال الفريق العامل لإدارة الانترنت مستمراً في عمله، في شكل منتدى دولي لقانون الانترنت، والذي يعتبر النواة الأولى لوضع النقاط الأساسية الأولى لتنظيم الانترنت بشكل عام وحرب المعلومات بشكل خاص وعقد عدة مؤتمرات أخرى في اليونان أثينا 2006 والبرازيل 2007 وإسلام آباد 2008 وشرم الشيخ 2009، غير أن هذه القمم لم تحقق التوقعات المرجوة منها وأخفقت في علاج كثير من القضايا المتعلقة بالفضاء الالكتروني المهمة، وخاصة فيما يتعلق بمساعدات الدول النامية التي تقدمها الدول الغنية للدول الفقيرة، وكما أن إعلان القمة العالمية لمجتمع المعلومات في جنيف 2003 وتونس 2005، كلها نصوص غير مفصلة وغير ملزمة إلا في القليل منها.

وأخيراً فإنه وأن كانت معظم أعمال المؤتمرات الدولية تأخذ شكل توصيات غير ملزمة للدول التي قد ترفض تنفيذها ولا توجد قوة حقيقية ملزمة لهذه التوصيات إلا أنها بتواترها وانسجامها مع بعضها البعض، فضلا عن إجماع الدول المشاركة فإنها تشكل اللبنة الأولى في بناء القانون الدولي للانترنت، فهي تساهم في نشأة قواعد عرفية جديدة في نطاق هذا القانون.

ثالثاً: الاتفاقية الأوربية للجرائم المرتكبة عبر الانترنت وحرب المعلومات Convention on Cybercrime 2001

سميت باتفاقية بودابست قد تم التوقيع عليها في تشرين الثاني 2001 ودخلت حيز التنفيذ في 1 أيلول 2004، صيغت هذه الاتفاقية من قبل الاتحاد الأوروبي سعيا منه إلى الحد من حركة الإجرام عبر الإنترنت، ولقد أضيف إلى هذه الاتفاقية بروتوكول معني بوضع نموذج لمكافحة جرائم الكراهية ضد الأجانب عبر الإنترنت وهو البروتوكول المسمى بروتوكول ستراسبورج المؤرخ 7 تشرين الثاني 2002 وضمت هذه الاتفاقية العديد من الدول الأوربية وغير الأوربية، وتلعب هذه الاتفاقية دوراً في تحسين التعاون الدولي في مجال مكافحة الجرائم عبر الفضاء الالكتروني والتركيز على تبني تشريعات مناسبة وطنية لتتلاءم مع الاتفاقية الدولية والتعريف بالجرائم المرتكبة عبر الفضاء الالكتروني وتحديد أركانها.

إلا أن أهم ما جاءت به الاتفاقية هو تحديد التعاريف

الهامة والضرورية في التعامل مع شبكة الانترنت "كمنظومة الكمبيوتر، وبيانات الكمبيوتر، ومزود الخدمة، وخط سير البيانات، في المادة الأولى من الفصل الأول، وقد تساعد هذه المصطلحات الالكترونية ضمن الصياغة الدولية في الاتفاقية الأوربية إلى اعتمادها، كمصطلحات قانونية دولية في الاتفاقيات الدولية المعتمدة عالمياً، وكذلك من خلال تحديدها إلى نوعية وأركان الجرائم التي قد ترتكب مثل جريمة "الدخول غير المشروع" والاعتراض غير المشروع وإساءة استخدام الأجهزة والتدخل الغير مشروع في المنظومة، في الفصل الثاني منها، وحل بعض التحديات التي تواجهنا في حرب المعلومات، مثل استخدام التعابير وشرح لبعض المصطلحات، وتحديد ماهية الجرائم التي قد تحدث في الانترنت، لذلك تعتبر هذه المعاهدة الدولية الأولى من شأنها تحديد الجرائم التي ترتكب عبر شبكة الإنترنت، ويمكن الركون إليها في تحديد معظم الجرائم التي قد ترتكب في حرب المعلومات، الفرع الثاني:

دور المنظمات الدولية

قامت منظمة الأمم المتحدة وكذلك المنظمات المتخصصة بدور فعال في مجال حماية الفضاء الالكتروني وتطوير القانون الدولي للانترنت، من خلال تبني استراتيجيات خاصة بهذا الشأن إلى جانب الأنشطة الأخرى التي تقوم بها، ومحاولة إعادة تفعيل دورها الرئيسي في حفظ الأمن والسلم الدوليين,ومن أجل صياغة معاهدة لمنع الحرب، والحاجة إلى معاهدة دولية بإشراف الأمم المتحدة.

أولا: دور منظمة الأمم المتحدة

لقد لعبت الأمم المتحدة دوراً بارزاً في صياغة القانون الدولي للانترنت سواء من خلال تنظيم مؤتمرات دولية حول تنظيم الفضاء الالكتروني، أو من خلال إنشاء الأجهزة والفرق واللجان والبرامج المعنية بحماية الفضاء الالكتروني، وتشجيع التعاون الدولي لصيانته أو من خلال إصدار القرارات والتوصيات التي تؤكد على مطالبة الحكومات بالتعاون الوثيق لوضع وتطبيق سياسة جماعية للتنمية الاقتصادية والاجتماعية من بين أهدافها تنظيم العمل في الفضاء الالكتروني.

وتعتبر مؤتمرات القمة العالمية لمجتمع المعلومات في جنيف 2003 وتونس 2005 والذي عقدا تحت مظلة الأمم المتحدة العمل التقني الأول في مجال القانون الدولي للفضاء الالكتروني، لكونه يحتوي على مجموعة من المبادئ المتعارف عليها لتنظيم العلاقة في مجال التعامل في الفضاء الالكتروني في الوقت الذي صدرت عنه. ومن الانجازات الهامة لمؤتمرات القمة كان تشكيل الفريق العامل المعني بإدارة الانترنت، والذي تمخض عنه فيما بعد "المنتدى حكم الانترنت Global Internet governance : كهيئة دولية مختصة، وتعقد الآن العديد من الندوات العالمية لمناقشة موضوع الأمن السيبراني تحت إشراف منظمة اليونيسكو وصدرت العديد من المؤلفات التي تنادي بضرورة إيجاد معاهدة دولية للانترنت ولحروب المعلومات.

الخلاصـــــة

تمثل حرب المعلومات حالياً مفهوماً جديداً تماماً من مفاهيم اللجوء إلى اتخاذ الإجراءات القسرية، وبالرغم من أنها لا تزال في المرحلة الأولى من العملية التطورية، إلا أنها قد وصلت بالفعل إلى النقطة التي لا بد من إخضاعها لنظام رقابي مصمم خصيصاً لمواجهة التحديات المعينة القائمة.

إن القواعد القانونية الدولية الحالية والمتعلقة باستخدام القوة بصورة عامة، والدفاع عن النفس بوجه خاص، يمكنها تنظيم الحرب الإلكترونية ولكن بشكل بسيط، حيث تم وضع تصور لمعالجة أقل أشكال العمل القسري الأكثر تقليدية، ولو أنها تعتبر الأمل الوحيد حالياً لتحقيق هذا التنظيم، في شكل مبدأ كارولين "Caroline Principle والذي إذا طبق في نهاية المطاف على أنها النظام التنظيمي الرئيسي في عمليات حرب المعلومات لا بد من أنه سوف يعقد الأمور، بدلا من يجعلها أكثر بساطة، لأنه أبعد من أن يكون قادراً على الإجابة عن التداخل السياسي، والقانوني، والتحديات الاقتصادية والعسكرية المختلفة التي أدخلها المفهوم الثوري للحرب الإلكترونية.

أوجدت هذه التحديات حالياً قواعد تتعلق بالدفاع عن النفس، وفشلت في مخاطبات عدة تحديات أخرى كانت قد واجهتها، وأنها تتطلب أجوبة دقيقة تنظيمية تكون ممكنة إذا أريد للسلام والأمن الدوليين أن يكونا مضمونين في العقود القادمة، واحتواء جميع التهديدات التي تتعلق بشن هجمات على الانترنت.

التحدي الأول من نوعه الذي فشل في التعامل مع القواعد القانونية الدولية التقليدية في الدفاع عن النفس كان مسألة المصطلحات المشتركة والمتجانسة، حيث ينطوي كل مفهوم جديد على مصطلح جديد حتماً. وتصبح هذه الحاجة أكثر إلحاحاً عندما ينطوي المفهوم الجديد على قضايا قانونية

وتكنولوجية معقدة، وهي بحاجة إلى التنظيم. كيف لنا ان نعرف هذا المفهوم الجديد وجميع الجوانب المتصلة به، والتي لديها تأثير مباشر على الإطار القانوني الفعلي وكيف سيتم تطبيقها على ذلك النظام الجديد، يجب عليه أن يكون هناك تنظيم محدد، وعلاوة على ذلك، وضع المصطلحات الصحيحة والتعريفات لهذه المفاهيم المتطورة حديثاً، مثل حرب الفضاء الإلكتروني ضروري جداً، وتبيان مدى تأثير بعض القضايا الأخرى على هذا المفهوم، مثل قضايا السياسة الجبرية، وتوفير التمويل الكافي لتطوير وسائل الدفاع اللازمة، أو حل المسائل التعاون بين جميع الوكالات الحكومية والأشخاص المسؤولين عنها قانونا للتعامل مع هذا الوضع الجديد، ليس فقط في داخل الدول ولكن أيضا على مستوى العلاقات بين الدول. المشكلة أكبر من ذلك فيما يتعلق بالإجراءات القسرية في الفضاء الإلكتروني نظرا للمضاعفات العديدة المتأصلة في هذا الشكل المعين من أشكال العمل القسري.

أولا، لأنه من الصعب التمييز بين الهجمات التي تقع على شبكات الحواسيب والتي قد تعزى إلى نشاط إجرامي عادي أو نشاط إرهابي أو حتى من الهجمات الواسعة النطاق من قبل دولة ما وهناك حاجة لتحديد فكرة "الهجوم المسلح" في الفضاء الإلكتروني. كما تبدو الأمور اليوم بوجود نقص في القواعد القانونية الدولية بوجه عام، والمبدأ القانوني الحالي للدفاع عن النفس بوجه خاص، ليس فقط وجود تعريف كاف للعمل الفعلي الذي يمكن تسميته 'هجوم الانترنت' ولكن أيضاً من خلال توافق في الآراء بشأن ما إذا كانت الهجمات على شبكات الحواسيب تشكل خطرا كافياً لتبرر بذل جهود متضافرة دفاعية ضد الهجوم من هذا القبيل وعلاوة على ذلك، هناك عدد قليل جداً من المصطلحات والتعاريف المتصلة بحرب الفضاء الإلكتروني التي يمكن أن تفسر بطرق مختلفة اعتماداً على من يستخدم هذا المصطلح بالفعل. على سبيل المثال، قد يكون مصطلح "monitoring" "الرصد أو المراقبة" قد يكون له معنى محدد للمؤسسة الدفاعية في بلد معين، ولكنه قد يكون له معنى آخر مختلف تماما إذا نظر إليه من خلال تطبيق القانون أو وجهة النظر القضائية، وأنه بالتأكيد لديه معنى آخر مختلف عندما نراه من وجهة نظر الحريات المدنية.

المسألة الثانية، التي تعتبر جزءاً لا يتجزأ من مجموعة الإمكانيات والجهود المتضافرة لتنظيم الهجمات على شبكات الحواسيب، والتي لا يتم تناولها من قبل القواعد القانونية القائمة في الدفاع عن النفس، هي حقيقة حرب الفضاء الإلكتروني وهي وجود المظهر العسكري والمدني. يتطلب الهجوم والدفاع في حرب المعلومات، على مستوى متساو تقريباً، علاقة عمل متقاربة جداً بين الدولة والقطاعين الخاص والعام، لأن تكنولوجيا المعلومات هي واحدة من الميادين القليلة التي يوجد فيها القطاع المدني من الناحية الفنية قبل العسكري. إذا كان لهذه العلاقة أن تنجح فإنه سيتعين أن ينظمها إطار قانوني مصمم خصيصاً لسد الفجوة التقليدية بين القطاع الخاص والحكومات الوطنية، وخصوصاً عندما يتعلق الأمر بالمشاريع الحر.

إن المحاولات التنظيمية المتعلقة بأنشطة حرب الفضاء الإلكترونية، لم يسبق لها مثيل بشأن التعاون فيما بين الدول، ويرجع هذا ليس فقط إلى حقيقة أن الشبكات العالمية يمكن الهجوم عليها ويمكن توجيه هذه الحرب عبر الحدود من قبل بلدان متعددة، ولكن أيضا ونتيجة لطبيعة الحرب الإلكترونية في التخفي بدقة، مما يجعل من الصعب للغاية بالنسبة للهجوم معرفة ما إذا كان موجهو الضربات هم من القراصنة العاديين أو هم من دولة أخرى. ولا بد من معالجة هذه المسألة بالذات ستكون ذات أهمية بالغة من وجهة النظر التنظيمية، وذلك لسبب آخر هو تعيين العتبة والمسؤولية القانونية التي قد تكون وراءه سواء أكانوا دولاً أم غير ذلك، والمبرر القانوني في اتخاذ الإجراءات القسرية للرد على هذه النشاطات الموجهة ضدهم.

ولا شك أن هناك بعض الجوانب من القانون الدولى التى يمكن تطبيقها على المسائل التى هي حالياً فى متناول اليد، إلا أنه ونظراً للطبيعة الخاصة جداً التى يتمتع بها الفضاء الالكترونى فإنه فضاء جديد تماماً، ويحتاج إلى تنظيم على درجة عالية من التخصص والتكامل لتحقيق المصالح الوطنية المختلفة المتعارضة بشدة. ونتيجة لذلك، هناك ضرورة قصوى تدعو وتحفز كل دول العالم للتحرك فى اتجاه اعتماد صك قانونى دولى مصمم خصيصاً لتنظيم قانون الإنترنت بشكل عام، وقانون لحرب المعلومات على وجه الخصوص، حتى تستطيع الدول ممارسة حقوقها فى استخدام القوة أو الدفاع عن النفس فى حال تعرضها لأي هجوم، وتطبيق ميثاق الأمم المتحدة بشكل دقيق ضماناً لتحقيق الأمن والسلم الدوليين.

الهوامش

(1) المقالةDepartment of Defense, 2004-pp31 et seq -40 مرفقة مع تعديلات البحث لسهولة الرجوع إليها–

(2) The Right To national self-Defence: in –J Elliston, information warfare operations -pp-45 et seq -47- at http://www.Parascope.com/ds/cyber1.htm (1999).

(3) J F Dunnigan, The Next War Zone: Confronting the Global Threat of Cyberterrorism, New York NY; Osborne/McGraw-Hill (2002)-pp200 et seq -224

(4) Joint Command, Control and Information Warfare School, Joint Information Operations Planning Handbook 118 (Washington DC: Joint Command, Control and Information Warfare School, 2003)pp-. V-14 et seq - V-20

(5) L J Freeh, Director of the FBI speech at the 1997 International Computer Crime Conference (March 4, 1997). Available at http://www.fbi.gov/dirspch/compcrim.htm–التقرير مرفق بالكامل مع تعديلات البحث –وقد أرفقته لصعوبة الاستحصال عليه من المتصفح العادي كونه من الملفات السرية المتعلقة بالدائرة الفيدرالية التحقيقية حول الجرائم التقنية الدولية.

(6) Dimitrios Delibasis, State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century Peace Conflict and Development: An Interdisciplinary Journal, Issue 8, February 2006-pp14-16

(7) B. Simma, "NATO, the UN and the Use of Force: "Legal Aspects", EJIL 10 (1999), 1 et seq. (11) –pp1-11

(8) Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, 'Protecting the Homeland', Report of the Defense Science Board Task Force on Defensive Information Operations: Memorandum for the Chairman, Defense Science Board 1 (Washington Volume II-March - DC: Department of Defense, 2001)-2001-pp12 et seq -15

(9) A Campen, D Dearth and R T Gooden Eds, Cyberwar: Security, Strategy and Conflict in the Information Age, Fairfax VA; AFCEA Press (1996).

(10) Y. Dinstein, War, Aggression and Self-Defense (Cambridge: Cambridge University Press, 2001)pp 170-173 and 174.

(11) C.C. Joyner/ C. Lotrionte, "Information Warfare as – International Coercion:Elements of a Legal Framework", EJIL 12 (2001)pp, 825 et seq. (827) (مما يدل على أن القواعد القانونية الموجودة في القانون المعاصر وميثاق الأمم المتحدة مفيدة ولكنها غير كافية للوصول إلى حلول مقبولة).

(12) W.G. Sharp, Sr., CyberSpace and the Use of Force, "Computer Attacks on Critical 1999, 7; E.T. Jensen, National Infrastructure: A Use of Force Invoking the Right of Self-Defense", Stanford J. Int'l L. 38 (2002), 207 et seq. (208).

(13) القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها قرارات، (1986) محكمة العدل الدولية A/56/ 770–

(14) Simma, NATO the UN and the Use of Force – Legal Aspects, 10 E.J.I.L. (1999). Ludwig Maximilians University of Munich - Faculty of Law- European Journal of International Law, Vol. 10, pp. 1-22, 1999

(15) D A Fulghum and R Wall, US Weather Operations in the Transformation Era - Air University Press Maxwell Air Force Base, Alabama-March 2003 at –pp-11-14-

(16) Charter of the United Nations, 59 Stat. 1031 T. S. No. 993, 3 Bevans 1153, Art. 51 (1945).

(17) Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, UN Doc. A/8028, General Assembly Resolution 2625, UN GAOR 25TH Session Supplement 28, 121 (1970).

(18) Definition of Aggression, UN Doc. A/9631, General Assembly Resolution 3314, UN GAOR 29TH Session Supplement 31, 142 (1974).

(19) Y. Dinstein, War, Aggression and Self-Defense 170-173 and 174 (Cambridge: Cambridge University Press, 2001). Also, US Department of Defense, Active Defense against Computer Intrusions 5-8 Washington – DC: Department of Defense, December 2nd 1998 pp14-26.

(20) D Chereshekin, V Tsygichko and G Smolyan, A Weapon That May Be More Dangerous than A Nuclear Weapon: The Realities of Information Warfare (1995).pp112-114 Available at: http://www.iwar.org.uk/iwar/resources/parameters/iw-deterrence.htm

(21) J F Dunnigan, The Next War Zone: Confronting the Global Threat of Cyberterrorism, New York NY; Osborne/McGraw-Hill (2002).).pp1-2

(22) D C Gompert, Right Makes Might: Freedom and Power in the Information Age, Institute for National Strategic Studies-- Strategic Appraisal: The Changing Role of Information in Warfare National Defense University Washington, DC, McNair Paper 59 (May 1998 -pp52-60.

(23) V ADM A K Cebrowski, Sea, Space, Cyberspace: Borderless Domains (1999). Available at http://www.nwc.navy.mil/press/speeches/borderless.htm

(24) د.محمود مرشحة–الوجيز في القانون الدولي العام– منشورات جامعة حلب–2008 - –ص112–115

(25) US Department of Defense – Office of the General Counsel, Active Defense against Peacetime Computer Intrusions 7 (Washington: Department of Defense, 1998).

(26) D C Gompert, National Security in the Information Age, Naval War College Review (Autumn 1998). Newport RI; Naval War College Press-pp22-25

(27) S T Hosmer, The Information Revolution and Psychological Effects, Santa Monica CA; Rand

(28) , Y. Dinstein, War, Aggression and Self-Defense 207-13 (Cambridge: Cambridge University Press, 2001)-pp12-23

(29) The Annotated Supplement to the Commander's Handbook on the Law of Naval Operations', U. S. Naval War College – Int'l Law Studies – Volume 73-pp- 290-292 (Annapolis VA: US Naval War College, 1997)

(30) Case Concerning United States Diplomatic and Consular Staff in Tehran, (1980) I. C. J. Rep. 3, 43.

(31) Tadic Case (The Verdict), (May 7, 1997) I.T. Press Release CC/PIO/190-E.

(32) البروتوكول (الأول)، الإضافيين لاتفاقيات جنيف المؤرخة في 12 أغسطس 1949 المتعلق بحماية ضحايا المنازعات الدولية المسلحة، UNJY 95-117. 4 و 43–51 (1977).

(33) L. C. Green, The Contemporary Law of Armed Conflictpp- 105-08 and 114-18 (Manchester: Manchester University Press, 2000).

(34) Tadic Case (The Verdict), (May 7, 1997) I.T. Press – Release CC/PIO/190-E

(35) A Rathmell, Strategic Information Warfare: Responding to the Threat, Centre for Defense studies, Brassey's Defense Yearbook (1998)-pp10-11

(36) L. C. Green, the Contemporary Law of Armed Conflict 268-72 and 274 (Manchester: Manchester University Press, 2000).pp2-3

(37) K W Quigley, A Framework for Evaluating the Legality of the United States Intervention in Nicaragua, 17 N.Y.U.J.I.L.P. (1985).

(38) A. Roberts and R. Guelff, Documents on the Laws of War 59 et seq. (Oxford: Oxford University Press, 2000).pp12-13

(39) J. P. Terry, (Colonel United States Marine Corps Ret.), 'Responding to Attacks on Critical Computer Infrastructure' XLVI Naval Law Review 170 et seq. (1999). Also, see generally, T. C. Wingfield, Legal Aspects of Offensive Information Operations in Space 2 et seq. (2003)-pp112-114 via http://www.usafa.mil/dfl/documents/wingfield.doc

(40) T. C. Wingfield, Legal Aspects of Offensive Information Operations in Space 1-4 (2003) via http://www.usafa.mil/dfl/documents/wingfield.doc

(41) Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 610 U.N.T.S. 205 (1967).

(42) P. A. Johnson (Colonel USAF/JAG Ret.), An Assessment of International Legal Issues in Information Operations 27. (Washington DC: Department of Defense, 1999).

(43) Agreement Relating to the International Telecommunications Satellite Organization, 23 U. S. T. 3813 (1971).

(44) Convention of the International Maritime Satellite Organization 31 U. S. T. 1 T. I. A. S. No. 9605 (1976).

(45) A Pearce, The Hague Conference and other International Conferences concerning the Laws and Usages of War: Text of Conventions with Notes, London; Stevens and Sons (1904).

(46) United Nations Conventions on the Law of the Sea". UN Doc. A/CONF.62/122, 21 I. L. M. 1261 (1982).

(47) United Nations Manual on the Prevention and Control of Computer Related Crime (2000). Available at http://www.ifs.univie.ac.at/~pr2gq1/rev434.html

(48) T. C. Wingfield, Legal Aspects of Offensive Information Operations in Space-pp 1-4 (2003) via http://www.usafa.mil/dfl/documents/wingfield.doc

(49) يمكن العودة للاستزادة : اتفاقية الاتصالات السلكية

والاسلكية الدولية، مع الملاحق والبروتوكولات، 6 تشرين الأول 1982 وثيقة المعاهدة 99-6 (1982) مجلس الشيوخ الأميركي

(50) D. J. Harris, Cases and Materials in International Law 765-70 (London: Thomson-Sweet and Maxwell, 2005)pp-12-22.

(51) L. C. Green, The Contemporary Law of Armed Conflict 57-8. (Manchester: Manchester University Press, 2000)-pp45-49

(52) A. D. McNair, 'The Functions and Differing Legal Character of Treaties', 11 B. Y. I. L. 100 (1930).

(53) The Chicago Convention "Chicago International Air Services Transit Agreement, U. K. T. S. 8 1953 Cmd. 8742 – 171 U.N. T. S. 387 Art. 3(d), 28 and 37 (1944).

(54) J. Adams, The Next World War: The Warriors and Weapons in the New Battlefields in Cyberspace 199 et seq. (London: Hutchinson, 1998). Also, J. F. Dunnigan, The Next War Zone: Confronting the Global Threat of Cyber terrorism 1 et seq. (New York NY: Osborne/McGraw-Hill, 2002).

(55) H. Thirlway, International Customary Law and Codification 4 et seq. (Lieden: A. W. Sijthoff, 1972).

(56) S.P. Kanuck, "Information Warfare: New Challenges for Public International Law", Harv. Int'l L. J. 37 (1996), 272 et seq. (286-287).

(57) Office of the Undersecretary of Defense – for Acquisition, Technology and Logistics, Protecting the Homeland: Report of the Defense Science Board on Defensive Information Operations 85 (Washington DC: Department of Defense, 2001).pp3-6

(58) G K Walker, Information Warfare and Neutrality, 33 Vanderbilt Journal of Transnational Law 1082 (2000).

(59) Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, Protecting the Homeland: Report of the Defense Science Board Task Force on Defensive Information Operations 85 et seq. (Washington DC: Department of Defense, 2001)

(60) Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, Protecting the Homeland: Report on the Defense Science Board Task Force on Defensive Information Operations 86 (Washington DC: Department of Defense, 2001)

(61) KAMAL A., 2005-The Law of Cyber-Space-Switzerland-United Nations Institute For Training and Research,197-254 Published by the United Nations Institute for Training and Research -Palais des Nations-CH 1211 Geneva 10-Switzerland-First Edition: October The Law of Cyber-Space- 2005-- KAMAL A., 2005-Switzerland- United Nations Institute For Training and Research-pp ,197-254.

(62) Antonio Segura-Serrano-., Internet regulation and the Role of International Law - Max Planck Yearbook of United Nations Law, Volume 10, 2006, p. 191-272-2006 Koninklijke Brill N.V. Printed in The Netherlands-pp22-32.

المصادر والمراجع

عيسى، وني، 2001، التنظيم القانوني لشبكة الانترنت (دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية)، منشورات صادر، ص92-99.

المجذوب، 2005، التنظيم الدولي-النظرية العامة والمنظمات العالمية والإقليمية والمتخصصة، منشورات الحلبي الحقوقية، ص211-214.

Simma. 1999. "NATO, the UN and the Use of Force: Legal Aspects", EJIL 10, I et seq., (11): 1-11.

Freeh. 1997. Director of the FBI speech at the 1997 International Computer Crime Conference. Available at http://www.fbi.gov/dirspch/compcrim.htm

Terry. 1999. (Colonel United States Marine Corps Ret.), 'Responding to Attacks on Critical Computer Infrastructure' XLVI Naval Law review 170 et seq. Also, see generally, T.C. Wingfield, Legal Aspects of Offensive Information Operations in Space 2 et seq. (2004) pp112-114 via http://www.usafa.mil/documents/wingield.doc

Wingfield. 2003. *Legal Aspects of Offensive Information Operations in Space* 1-4 et seq. (2003) via http://www.usafa.mil/documents/wingield.doc

Thirlway. 1972. International Customary Law and Codification 4 et seq. (Lieden: A.W. sijthoff).

Kanuck. 1996. "Information Warfare: New challenges for Public International Law", Harv. Int'l L. J. 37, 272 et seq. (286-287).

Office of the Undersecretary of Defense- for Acquisition, Technology and Logistics, Protecting the Homeland: Report of the Defense Science Board on Defensive Information Operations 85 (Washington DC: Department of Defense) pp3-6.

Walker. 2000. Information Warfare and Neutrality, 33 Vanderbilt Journal of Transnational Law 1082.

The Rights and Obligations of the States in the Information's War

Moustafa Na'os*

ABSTRACT

This study begins with a short overview of the various aspects of cyberspace warfare in an attempt to make clear the new form of war which represents to international peace and security. It then moves on to examine cyberspace warfare within the context of currently existing international legal norms on the use of force and to determine if these norms can be applied to this new form of warfare and if so, to what extent. Finally, the essay attempts to make apparent a twofold fact: first, that current legal norms on the use of force can only be applied to cyberspace by analogy and up to a certain point, hence there is a need to develop a regulatory framework specifically tailored for this purpose; second that the cause behind this need is the 'special' nature of cyberspace warfare.

Keywords: Cyberspace Warfare-International Peace and Security- Use of Force for Self-Defence.

* Lawyer, The Bar Association, Aleppo, Syria. Received on 11/7/2010 and Accepted for Publication on 13/4/2013.